ATKIN AND SWINNERTON-DYER CONGRUENCES AND NONCONGRUENCE MODULAR FORMS

WEN-CHING WINNIE LI AND LING LONG

Abstract. Atkin and Swinnerton-Dyer congruences are special congruence recursions satisfied by coefficients of noncongruence modular forms. These are in some sense p-adic analogues of Hecke recursion satisfied by classic Hecke eigenforms. They actually appeared in different context and sometimes can be obtained using the theory of formal groups. In this survey paper, we introduce the Atkin and Swinnerton-Dyer congruences, and discuss some recent progress on this topic.

1. Introduction

Atkin and Swinnerton-Dyer (ASD) congruences in the title refer to the congruences of the form

$$a_{np} - A_p a_n + \mu_p p^{k-1} a_{n/p} \equiv 0 \mod p^{(k-1)(1+ord_p n)} \quad \text{for all n} \geq 1, \tag{1}$$

where p is a prime, a_n are p-adically integral, A_p is an algebraic integer, and μ_p is a root of unity. As usual, $a_x = 0$ if x is not an integer. The original purpose was to study the arithmetic properties of the Fourier coefficients $a_n = a_n(f)$ of a weight-k cusp form f for a finite index subgroup Γ of $SL_2(\mathbb{Z})$. When Γ is a congruence subgroup and f is an eigenfunction of the Hecke operator at p, then with A_p being the eigenvalue and congruence replaced by equality, this is the familiar three term recursive relation. When Γ is a noncongruence subgroup, which is the majority, such f may be regarded as playing the role of a Hecke eigenfunction at p. This remarkable observation was made by Atkin and Swinnerton-Dyer in their seminal paper [ASD71], which initiated a systematic study of the arithmetic of noncongruence modular forms. Assume that the modular curve of Γ has a model defined over $\mathbb{Q}$ such that the cusp at infinity is $\mathbb{Q}$-rational, $k \geq 2$ and the space $S_k(\Gamma)$ of weight-k cusp forms for Γ is d-dimensional. Based on their numerical evidence, Atkin and Swinnerton-Dyer expected $S_k(\Gamma)$ to contain a basis with this congruence property for good primes p, although the basis would vary with p. Using the degree-$2d$ Galois representations attached to $S_k(\Gamma)$, Scholl in [Sch85] proved that such a basis exists at primes p where the action of the Frobenius has d distinct p-adic unit eigenvalues. In §6.3, we give some examples of $S_k(\Gamma)$ for which the ASD expectation holds for almost all primes and also an example where the ASD congruence fails for half of the primes. In the paper [Sch85] Scholl also showed that all forms f in $S_k(\Gamma)$ with p-adically integral Fourier coefficients satisfy a similar, but longer, $(2d+1)$-term congruence for all $n \geq 1$:

$$a_{np^d}(f) + A_1 a_{np^{d-1}}(f) + \cdots + A_d a_n(f) + \cdots + A_{2d} a_{n/p^d}(f) \equiv 0 \mod p^{(k-1)(1+ord_p n)}.$$

Here $T^{2d} + A_1 T^{2d-1} + \cdots + A_{2d} \in \mathbb{Z}[T]$ is the characteristic polynomial of the geometric Frobenius at p under the Galois representation. See §2 for details.

Very recently, Kazalicki and Scholl [KS13] extended the above congruence to include weakly holomorphic exact weight-k cusp forms for Γ, but with weaker modulus $p^{(k-1)ord_p n}$ instead. This

The first author is supported by the NSF grant DMS-1101368. The second author is supported by NSF grant DMS-1001332. Part of the material was based on the talk given by the first author at RIMS on Dec. 5, 2012. This paper was written while the second author was visiting Cornell University as an AWM Michler scholar. She is in debt to both AWM and Cornell University. The computations were made using the mathematical software Sage, special thanks to the Sage Group.

is discussed in §6. In §7, we describe an application of the ASD congruences to an open conjecture characterizing genuine noncongruence modular forms.

The congruences discovered by Atkin and Swinnerton-Dyer actually also appeared in different context. For instance, when the modulus is $p^{1+ord_p n}$ (with $k = 2$), the ASD type congruences can be obtained using the theory of formal groups, recalled in §3. These congruences are closely related to Dwork's work on p-adic hypergeometric series, see §4. Section 5 is devoted to some geometric backgrounds for ASD congruences, including p-adic analogues of the Selberg-Chowla formula and solutions of certain ordinary differential equations. Meanwhile, we exhibit some known and some conjectural supercongruences, which are ASD type congruences that are stronger than what can be predicted from the formal group laws. We end the paper by discussing another type of congruences discovered by Atkin, which led to the development of p-adic modular forms.

2. Congruence and noncongruence modular forms

2.1. **Finite index subgroups of $SL_2(\mathbb{Z})$, modular curves, and modular forms.** It is well-known that all finite index subgroups of $SL_n(\mathbb{Z})$ for $n \geq 3$ are congruence subgroups (cf. [BLS64, BMS67]). This property no longer holds for the modular group $SL_2(\mathbb{Z})$. In fact, among its finite index subgroups, noncongruence ones out number the congruence ones. One way to see this is from the defining fields of the associated modular curves. More precisely, the modular curve X_Γ of a finite index subgroup Γ of $SL_2(\mathbb{Z})$ is a Riemann surface obtained as the orbit space of the action of Γ on the Poincaré upper half-plane via fractional linear transformations, compactified by adding finitely many cusps. It is known to have a model defined over a number field. When Γ is a congruence subgroup $\Gamma_0(N)$ or $\Gamma_1(N)$, the modular curve is defined over $\mathbb{Q}$, and for the principal congruence subgroup $\Gamma(N)$, its modular curve has a model defined over the cyclotomic field $\mathbb{Q}(e^{2\pi i/N})$. On the other hand, a celebrated result of Belyĭ asserts that

Theorem 1 (Belyĭ, [Bel79]). *A smooth irreducible projective curve defined over a number field is isomorphic to a modular curve X_Γ for (infinitely many) finite index subgroup(s) Γ of $SL_2(\mathbb{Z})$.*

Thus simply by considering curves defined over number fields one sees easily that $SL_2(\mathbb{Z})$ contains far more noncongruence subgroups than congruence ones.

Given a finite index subgroup Γ of $SL_2(\mathbb{Z})$, recall that a weight-k modular form for Γ is a holomorphic function f on the upper half-plane satisfying

$$f(z) = (cz+d)^{-k} f\left(\frac{az+b}{cz+d}\right) \quad \text{for all } \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma,$$

and the extra condition that f is holomorphic at the cusps of Γ. It is called a cusp form if it vanishes at all cusps of Γ. We call it a congruence form if it is for a congruence subgroup; otherwise it is called a noncongruence form. Denote by $M_k(\Gamma)$ (resp. $S_k(\Gamma)$) the space of all weight-k modular forms (resp. cusp forms) for Γ.

When $k = 2$, the forms $f \in S_2(\Gamma)$ may be identified with the holomorphic differential 1-forms $f(z)dz$ of X_Γ. The de Rham space $H^1(X_\Gamma, \mathbb{C})$ is $2g$-dimensional, where g is the genus of X_Γ, consisting of holomorphic and anti-holomorphic 1-forms of X_Γ; these two spaces are dual to each other with respect to the cup product on $H^1(X_\Gamma, \mathbb{C})$.

2.2. **Congruence modular forms.** The arithmetic for congruence forms is well-understood, after being studied for over one century. The two main ingredients are the Hecke theory and l-adic Galois representations. The newform theory says that it suffices to study the arithmetic of newforms of weight k, level N, and character χ [AL70, Mik71, Li75]. Such a form f is a common eigenfunction of the Hecke operators at the primes p not dividing N. The Fourier coefficients $a_n(f)$ of f with the leading coefficient $a_1(f) = 1$ are algebraic integers satisfying

$$a_{mn}(f) = a_m(f)a_n(f) \qquad \text{for } (m,n) = 1,$$

and the 3-term recursive relation

$$a_{np}(f) - a_p(f)a_n(f) + \chi(p)p^{k-1}a_{n/p}(f) = 0 \qquad \text{for all } p \nmid N \text{ and all } n \geq 1. \tag{2}$$

The work of Eichler-Shimura [Shi71] (for $k = 2$) and Deligne [Del69] (for $k \geq 3$) associates to f a compatible family of degree two l-adic representations $\rho_{l,f}$ of the absolute Galois group $G_{\mathbb{Q}}$ over $\mathbb{Q}$, unramified outside lN such that the characteristic polynomial of $\rho_{l,f}$ at the Frobenius at $p \nmid lN$ has characteristic polynomial $H_p(T) = T^2 - a_p(f)T + \chi(p)p^{k-1}$. As a consequence, one concludes that $|a_p(f)| \leq 2p^{k-1}$ holds for all $p \nmid N$. The above developments originated from Ramanujan's observations on the discriminant Delta function in $S_{12}(SL_2(\mathbb{Z}))$

$$\Delta(z) := \eta(z)^{24} = q\prod_{n\geq 1}(1-q^n)^{24} = \sum \tau_n q^n, \quad \text{where } q = e^{2\pi i z}.$$

2.3. **Noncongruence modular forms.** In comparison, modular forms for noncongruence subgroups are far more mysterious than their congruence counterparts due to the lack of effective Hecke operators, which was conjectured by Atkin and proved by Serre [Tho80] for noncongruence subgroups normal in $SL_2(\mathbb{Z})$ and Berger [Ber94] in general. More precisely, if one mimics what's done for congruence forms by defining a Hecke operator at p for a noncongruence subgroup Γ by using the Γ-double coset represented by a 2×2 matrix with entries in $\mathbb{Z}$ and determinant p, then, as shown in [Ber94], this operator is the composition of the trace map from Γ to Γ^c, the smallest congruence subgroup containing Γ, followed by the usual Hecke operator at p on Γ^c. Unfortunately the trace map annihilates all genuine noncongruence forms, hence no information can be drawn for the noncongruence forms we are interested in.

However, it is not difficult to construct noncongruence modular forms as long as we keep an eye on the ramification. For weight 0 modular forms, namely *modular functions*, we have

Theorem 2 (Atkin and Swinnerton-Dyer, [ASD71])**.** *An algebraic function of the (modular) j-function is a modular function if and only if, as a function of j-function, it only ramifies at 3 points 1728, 0 and infinity with ramification indices 2, 3, and arbitrary, respectively.*

A systematic investigation on noncongruence modular forms was initiated by the work of Atkin and Swinnerton-Dyer [ASD71]. They showed some similarities between congruence and noncongruence forms. Given a finite index subgroup Γ of $SL_2(\mathbb{Z})$, for convenience, assume that the modular curve X_Γ has a model defined over $\mathbb{Q}$ under which the cusp ∞ is a $\mathbb{Q}$-rational point. Then there is an integer M depending on Γ and the model of X_Γ such that $S_k(\Gamma)$ contains a basis whose Fourier coefficients are integral over $\mathbb{Z}[\frac{1}{M}]$, see [Sch85]. Suppose $k \geq 2$ is even and $S_k(\Gamma)$ has dimension d. From their numerical examples, Atkin and Swinnerton-Dyer observed that for good primes p, the space $S_k(\Gamma)$ possesses a basis $\{f_i\}_{1\leq i\leq d}$ with p-adically integral Fourier coefficients $a_n(f_i)$ and for each i there exists an algebraic integer $A_p(i)$ with $|A_p(i)| \leq 2p^{(k-1)/2}$ such that

$$a_{np}(f_i) - A_p(i)a_n(f_i) + p^{k-1}a_{n/p}(f_i) \equiv 0 \mod p^{(k-1)(1+\mathrm{ord}_p n)}, \quad \forall n \geq 1. \tag{3}$$

The striking similarity between this and (2) suggests that the p-adic theory for noncongruence modular forms could be fruitful as well.

To understand what Atkin and Swinnerton-Dyer discovered, Scholl in [Sch85] constructed Galois representations attached to the space $S_k(\Gamma)$ by extending the construction of Deligne. He proved that there exists a compatible family of $2d$-dimensional l-adic Galois representations ρ_l of the Galois group $G_{\mathbb{Q}}$ unramified outside lM such that for any prime $p \nmid lM$ the characteristic polynomial of the geometric Frobenius under ρ_l is a degree $2d$ polynomial $H_p(T) = T^{2d} + A_1T^{2d-1} + \cdots + A_{2d}$ with coefficients in $\mathbb{Z}$ and all roots of the same absolute value $p^{(k-1)/2}$. In fact, $H_p(T)$ can be computed by explicit formulas of counting points on elliptic curves over finite fields. Moreover, by a comparison theorem between étale and crystalline cohomologies, Scholl proved that for $p > k-2$ and $p \nmid M$, any $f \in S_k(\Gamma)$ with p-adically integral Fourier coefficients $a_n(f)$ satisfies the congruence

$$a_{np^d}(f) + \cdots + A_d a_n(f) + \cdots + A_{2d}a_{n/p^d}(f) \equiv 0 \mod p^{(k-1)(1+\mathrm{ord}_p n)}, \quad \forall n \geq 1. \tag{4}$$

In particular, when $H_p(T)$ has d distinct p-adic unit roots, the above long congruence can be reduced to 3-term congruences satisfied by a basis of $S_k(\Gamma)$, as observed by Atkin and Swinnerton-Dyer.

Scholl representations are of motivic nature. According to the Langlands philosophy, the L-functions of Scholl's representations should coincide with L-functions of automorphic representations of certain reductive groups. The congruences (3) and (4) can then be interpreted as congruence relations between Fourier coefficients of noncongruence forms and those of automorphic forms. For 2-dimensional Scholl representations of $G_{\mathbb{Q}}$, their modularity follows from a renowned conjecture of Serre established by Khare and Wintenberger [KW09] and various modularity lifting theorems [SW99, SW01, DM03, DFG04, Kis09a, ALLL, et al.]. What makes Scholl representations interesting is that they cannot be decomposed into degree-2 pieces in general and hence provide a fertile testing ground for Langlands philosophy. For more details in this regard, see a survey [Li12]. In §7, we will give an application of the ASD congruences as well as the automorphy of Scholl representation [LL12]. In the proof, we also used the best known bound for the coefficients of noncongruence cusp forms obtained by Selberg, with saving 1/5 (instead of 1/2). It is unclear whether coefficients of noncongruence cusp forms will satisfy the Ramanujan-Petersson conjecture.

To illustrate the above results we exhibit an example below. Let $\Gamma^1(5)$ be the group consisting of matrices in $SL_2(\mathbb{Z})$ which become lower triangular unipotent when modulo 5. It has 4 cusps, ∞, 0, -2, and $-5/2$, and admits a normalizer $A = \begin{pmatrix} -2 & -5 \\ 1 & 2 \end{pmatrix}$ which swaps cusps ∞ and -2. Let E_1, E_2 be weight-3 Eisenstein series of $\Gamma^1(5)$, which have simple zeros at all cusps except ∞ and -2, respectively, and nonvanishing elsewhere. Both of them have integer Fourier coefficients:

$$\begin{aligned} E_1(z) &= 1 - 2q^{1/5} - 6q^{2/5} + 7q^{3/5} + 26q^{4/5} + \cdots, \\ E_2(z) &= q^{1/5} - 7q^{2/5} + 19q^{3/5} - 23q^{4/5} + \cdots. \end{aligned}$$

For more details, see [LLY05, §4]. Thus $t = \frac{E_2}{E_1}$ is a modular function for $\Gamma^1(5)$ with a simple zero and a simple pole, both located at the cusps. By Theorem 2, $\sqrt{t}$ is a modular function for an index-2 subgroup Γ_2 of $\Gamma^1(5)$. Also,

$$f = E_1 t = \sqrt{E_1 E_2} = \sum a_n q^{n/10} = q^{1/10} - \frac{3^2}{2} q^{3/10} + \frac{3^3}{2^3} q^{5/10} + \frac{3 \cdot 7^2}{2^4} q^{7/10} + \cdots$$

is a weight-3 cusp form for Γ_2, which in fact generates $S_3(\Gamma_2)$. The group Γ_2 is a noncongruence subgroup because the Fourier coefficients of $\sqrt{E_1E_2}$ have unbounded denominators. No congruence cusp form behaves this way, since it is a linear combination of Hecke eigenforms, whose Fourier coefficients are algebraic integers. This distinction is conjectured to be a criterion to distinguish congruence forms from genuine noncongruence forms with algebraic Fourier coefficients. This conjecture is of fundamental importance and is very useful in many applications. It will be discussed later in §7. Nevertheless, coefficients of noncongruence modular forms are almost integral, if they are algebraic.

For $S_3(\Gamma_2)$ the ASD congruences proved by Scholl asserts that, for all primes $p > 3$, there are A_p, B_p in $\mathbb{Z}$ such that

$$a_{np^r}(f) - A_p a_{np^{r-1}}(f) + B_p a_{np^{r-2}}(f) \equiv 0 \mod p^{2r}, \quad \forall n, r \geq 1.$$

In particular, the corresponding 2-dimensional l-adic Scholl representation of $G_{\mathbb{Q}}$ is reducible when restricted to $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(i))$ due to the involution induced by the A-operator on the representation space. Consequently, one can checked that A_p agrees with the pth coefficient of the weight-3 Hecke eigenform $\eta(4z)^6 = q\prod_{n\geq 1}(1-q^{4n})^6$ and $B_p = (-1)^{(p-1)/2}p^2$. For more details, see [LLY05].

3. ASD congruences and 1-dimensional commutative formal group laws

3.1. **ASD congruences for elliptic curves.** The inspiration of the congruence (3) observed by Atkin and Swinnerton-Dyer came from what they proved for weight-2 cusp forms for Γ of genus one. In this case the modular curve X_Γ is an elliptic curve $E:\ y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Let $p > 3$ be a prime such that E has good reduction modulo p. Let ξ be a local uniformizer of E at the point at infinity which is either $-\frac{x}{y}$ or $-\frac{x}{y}$ plus higher order terms with coefficients in $\mathbb{Z}$. The coefficients of the holomorphic differential 1-form $\frac{dx}{2y} = \sum_{n\geq 1} a_n \xi^n \frac{d\xi}{\xi}$ satisfy

$$a_{np^r} - (p + 1 - \#[E/\mathbb{F}_p])a_{np^{r-1}} + pa_{np^{r-2}} \equiv 0 \mod p^r, \quad \forall n, r \geq 1. \tag{5}$$

This can be explained by using 1-dimensional commutative formal group law, which we will recall in the next section by following the development in [Kib11]. For more information on d-dimensional commutative formal group laws, the reader is referred to [Haz78, Dit90, Kib11].

3.2. **1-dimensional commutative formal group law (1-CFGL).** A 1-CFGL over a characteristic 0 commutative integral domain R with units, such as $\mathbb{Z}$, $\mathbb{Z}[1/M]$, or $\mathbb{Z}_p$, is a formal power series $G(x, y)$ in $R[[x, y]]$ satisfying

- $G(x, y) = x + y + \sum_{i,j\geq 1} c_{i,j} x^i y^j, c_{i,j} \in R$,
- (Associativity) $G(x, G(y, z)) = G(G(x, y), z)$,
- (Commutativity) $G(x, y) = G(y, x)$.

Corresponding to each formal group is a unique normalized *invariant differential*

$$\omega(v) = [\partial_u G(0, v)]^{-1} dv = 1 + \sum_{n\geq 2} a_i v^{i-1} dv, a_i \in R$$

where ∂_u means partial derivative with respect to the first variable. The corresponding *strict formal logarithm* is defined to be

$$\ell(v) := \int \omega = v + \frac{a_2}{2} v^2 + \frac{a_3}{3} v^3 + \cdots$$

so that $G(u, v) = \ell^{-1}(\ell(u) + \ell(v))$.

Two 1-CFGLs $G(x, y)$ and $\bar{G}(x, y)$ over R are said to be *isomorphic* if there exists a formal power series $\phi(x) = ax+$higher terms in $R[[x]]$ with $a \in R^\times$ such that $\phi(G(x, y))) = \bar{G}(\phi(x), \phi(y))$. If $a = 1$, then the isomorphism is said to be *strict*. Thus, over the field of fractions of R, each 1-CFGL is strictly isomorphic to the additive CFGL $G(x, y) = x + y$ via the formal logarithm.

Proposition 3. *If $f(x) = \sum \frac{a_n}{n} x^n$ is the strict formal logarithm of a 1-CFGL $G(x, y)$ over R, then for any $\phi(x) = x +$ higher terms $\in R[[x]]$, $f(\phi(x)) = \sum \frac{b_n}{n} x^n$ is the strict formal logarithm of a 1-CFGL, which is strictly isomorphic to $G(x, y)$.*

Denote by S the set of formal power series of the form $f = \sum_{n\geq 1} \frac{a_n}{n} x^n$ with $a_n \in R$. It is an R-module. On S we define the following operators with integers $m \geq 1$ and $\lambda \in R$:

- (*Frobenius*) $F_m f(x) = \sum_{n\geq 1} \frac{a_{mn}}{n} x^n$,
- (*Verschiebung*) $V_m f(x) = \sum_{n\geq 1} \frac{a_n}{n} x^{mn}$,
- (*Witt operator*) $[\lambda] f(x) = \sum \frac{a_n}{n} \lambda^n x^n$.

Note that $[\lambda]f(x)$ corresponds to the change of variable $x \mapsto \lambda x$. Thus any formal group isomorphism can be decomposed into a strict isomorphism followed by a Witt operator. Endow the x-adic topology on S so that the open neighborhood system of $f \in S$ consists of $U_{f,n} := \{g \in S \mid g \equiv f (\text{mod degree } n)\}$ for $n \geq 1$. The completion of the R-module generated by the Frobenius, Verschiebung, and Witt operators is the called the *Cartier Module*.

The following theorem characterizes the strict formal logarithms for a 1-CFGL.

Theorem 4. *$f \in S$ is the strict formal logarithm for a 1-CFGL over R if and only if for each prime p there exist $\lambda_{p,i} \in R$ such that*

$$F_p f = \sum_{i \geq 1} V_i[\lambda_{p,i}] f.$$

For the remaining discussion, assume that for any maximal ideal $\wp$ of R with residual characteristic p, the completion of the localization of R at $\wp$ is an unramified ring extension of $\mathbb{Z}_p$. Let $\sigma(\wp)$ be the ring automorphism sending $r \in R$ to $r^{\sigma(\wp)} \equiv r^p \mod \wp$. On the submodule S_p of S of formal power series of the form $g = \sum_{i \geq 0} \frac{a_{p^i}}{p^i} x^{p^i}$, for each $\mu \in R$ we define the *Hilbert operator* $\{\mu\}$: it sends g to $(\{\mu\} g) = \sum \frac{a_{p^i}}{p^i} \mu^{\sigma(\wp)^i} x^{p^i}$. Then the Witt operators on S_p are generated by F_p, V_p and the Hilbert operators.

Theorem 5. *Suppose $f = \sum_{n \geq 1} \frac{a_n}{n} x^n \in S$ is the strict formal logarithm of a 1-CFGL over R as above. Then for each residual characteristic p of a maximal ideal of R, there are $\mu_{p,i} \in R$ such that*

$$F_p f_{(p)} = \sum_{i \geq 0} V_{p^i} \{\mu_{p,i}\} f_{(p)}, \quad \textit{where } f_{(p)} = \sum_{i \geq 0} \frac{a_{p^i}}{p^i} x^{p^i}.$$

The above expression is called the Hilbert F_p-type for f.

The theorem above asserts the following relation on coefficients of $f_{(p)}$:

$$a_{p^{n+1}} = \sum_{i=0}^{n} p^i a_{p^{n-i}} \mu_{p,i}^{\sigma(\wp)^{n-i}} = \sum_{i=0}^{n} p^i \mu_{p,i} a_{p^{n-i}}^{\sigma(\wp)^{i+1}},$$

where the last equality is due to the commutativity relation $\{\mu\} V_p = V_p \{\mu^{\sigma(\wp)}\}$ and $\sigma(\wp)$ being a ring automorphism of R. This leads to the following general congruences:

$$a_{mp^{n+1}} \equiv \sum_{i=0}^{n} p^i \mu_{p,i} a_{mp^{n-i}}^{\sigma(\wp)^{i+1}} \mod \wp^{n+1}, \quad \forall\, n, m \geq 1. \tag{6}$$

When $a_p \not\equiv 0 \mod \wp$, i.e. p is ordinary for the 1-CFGL, there exists a $\wp$-adic unit α_p such that

$$a_{mp^{n+1}} \equiv \alpha_p a_{mp^n} \mod \wp^{n+1}, \quad \forall\, n, m \geq 1. \tag{7}$$

Theorem 6. *If two 1-CFGLs over R are strictly isomorphic, then their formal logarithms satisfy the same Hilbert F_p- type for any unramified maximal ideal $\wp$ of R.*

3.3. **ASD congruences for elliptic curves continued.** To resume our discussion in §3.1, one can construct a formal group associated to the elliptic curve $E : y^2 = x^3 + Ax + B$ as follows. In a neighborhood V of the point at infinity, each point $P = (x, y)$ on E is marked by $\xi(P) = -\frac{x}{y}$. Given P_1, P_2 in V, one can compute $P_3 = P_1 + P_2$ under the group law on E and expresses $\xi(P_3)$ as a formal power series in $\xi(P_1)$ and $\xi(P_2)$ with coefficients in $\mathbb{Z}[\frac{1}{6}]$. This formal power series satisfies all axioms of the 1-CFGL with $\frac{dx}{2y}$ expanded in powers of $\xi = -\frac{x}{y}$ as its invariant differential. Namely, $\frac{dx}{2y}$ gives rise to a 1-CFGL over $\mathbb{Z}[\frac{1}{6}]$ which is naturally identified with the infinitesimal group law of the elliptic curve around the point at infinity. Honda [Hon68] proved that this formal group is strictly isomorphic to the formal group constructed from the L-function $L(E, s) = \sum_{n \geq 1} b_n n^{-s}$ of $E/\mathbb{Q}$. Thus both group laws yield congruence relations with the same $\mu_{p,0}, \mu_{p,1}, \cdots$ by Theorem 6. It follows from the definition of $L(E, s)$ as an Euler product that its coefficients b_n satisfy the relation $b_p = p + 1 - \#[E/\mathbb{F}_p]$ and

$$b_{np} - b_p b_n + p b_{n/p} = 0, \quad \forall\, n \geq 1$$

for all primes p not dividing the conductor N of E. For such p we have $\mu_{p,0} = b_p$, $\mu_{p,1} = -1$ and $\mu_{p,j} = 0$ for $j \geq 2$ so that (5) holds.

4. ASD type congruences and Dwork's result

4.1. **ASD congruences for Legendre family of elliptic curves.** For a nonnegative integer r and $\alpha_i, \beta_i \in \mathbb{C}$, the hypergeometric series ${}_{r+1}F_r$ is defined by

$$ {}_{r+1}F_r\begin{bmatrix} \alpha_1 & \dots & \alpha_{r+1} \\ \beta_1 & \dots & \beta_r \end{bmatrix}; x \Bigg] = \sum_{k=0}^{\infty} \frac{(\alpha_1)_k(\alpha_2)_k\dots(\alpha_{r+1})_k}{(\beta_1)_k\dots(\beta_r)_k}\cdot\frac{x^k}{k!}, $$

which converges for $|x|<1$. It is well-known that this series satisfies a degree-r ordinary differential equation in x. Denote by ${}_{r+1}F_r\left[\begin{matrix} \alpha_1 & \dots & \alpha_{r+1} \\ \beta_1 & \dots & \beta_r \end{matrix}; x\right]_n$ the truncation of the series after the x^n term.

Let $E_\lambda : y^2 = x(x-1)(x-\lambda)$ be the Legendre family of elliptic curves. Its Picard-Fuchs equation is a degree-2 hypergeometric differential equation with the unique holomorphic solution near zero (up to scalar multiples) to be ${}_2F_1(\begin{smallmatrix}\frac12, \frac12\\ 1\end{smallmatrix}; \lambda)$. Expand $\omega = \frac{dx}{2\sqrt{x(x-1)(x-\lambda)}} = \sum \frac{a_n}{n}\xi^n\frac{d\xi}{\xi}$ with $\xi = -\frac{x}{y}$. Using a formula due to Beukers (see [Dit90, pp. 272]), a_n is the $(n-1)$st coefficient of x in $(x(x-1)(x-\lambda))^{\frac{n-1}{2}}$. Thus

$$ a_{2k+1} = {}_2F_1(\begin{smallmatrix}-k, -k\\ 1\end{smallmatrix}; \lambda)(-1)^k = {}_2F_1(\begin{smallmatrix}-k, 1+k\\ 1\end{smallmatrix}; \tfrac{-\lambda}{1-\lambda})(\lambda-1)^k. \tag{8} $$

As $-k$ is a negative integer, the above hypergeometric series terminates at x^k. When $\lambda \in \mathbb{Q}$, the ASD congruence (5) for ordinary prime p is equivalent to

$$ \frac{{}_2F_1\left(\begin{matrix}\frac{1-p^s}{2}, \frac{1\pm p^s}{2}\\ 1\end{matrix}; \lambda\right)}{{}_2F_1\left(\begin{matrix}\frac{1-p^{s-1}}{2}, \frac{1\pm p^{s-1}}{2}\\ 1\end{matrix}; \lambda\right)} \equiv \left(\frac{-1}{p}\right)\beta_{p,\lambda} \pmod{p^s}, \tag{9} $$

where $\beta_{p,\lambda}$ is the unit root of $T^2-(p+1-\#[E_\lambda/\mathbb{F}_p])T+p$ and hence only depends on the residue of λ in $\mathbb{F}_p$. For details, see [KLMSY].

We proceed to compare the above with some results of Dwork. Let p be a fixed prime. For any $a\in\mathbb{Z}_p$, denote by a' be the unique number in $\mathbb{Z}_p$ such that $pa'-a\in\{0,1,\cdots,p-1\}$. For instance, when p is odd, $(\frac12)' = \frac12$.

Theorem 7 (Dwork, [Dwo69])**.** *Let K be a complete p-adic field with the ring of integers R. Let $A(n) := B^{(-1)}(n), B(n) := B^{(0)}(n), B^{(1)}(n), \cdots$ be R-valued sequences of arithmetic functions obtained from consecutive applications of $'$. Let $F(X) := \sum_{n\ge0} A(n)X^n$ and $G(X) := \sum_{n\ge0} B(n)X^n$. Suppose that for all integers $n, m, s \ge 1, i\ge -1$,*

(1) *$B^{(i)}(0)$ is a unit in R;*
(2) $\frac{B^{(i)}(n)}{B^{(i)}([\frac{n}{p}])} \in R$*;*
(3) $\frac{B^{(i)}(n+mp^{s+1})}{B^{(i+1)}([\frac{n}{p}]+mp^s)} \equiv \frac{B^{(i)}(n)}{B^{(i+1)}([\frac{n}{p}])} \mod p^{s+1}$.

Then

$$ F(X)\sum_{j=mp^s}^{(m+1)p^s-1} B(j)X^{pj} \equiv G(X^p)\sum_{j=mp^{s+1}}^{(m+1)p^{s+1}-1} B(j)X^j \mod B^{(s)}(m)p^{s+1}[[X]]. $$

Intuitively, the condition (3) is about certain p-adic continuity of $\frac{B^{(i)}(n)}{B^{(i+1)}([\frac{n}{p}])}$, as a function of n. It is satisfied by the p-adic (Morita) Gamma function $\Gamma_p(x)$, which is a function from $\mathbb{Z}_p$ to $\mathbb{Z}_p^\times$ such that for any $x\in\mathbb{Z}_p$, $\Gamma_p(x+1)/\Gamma_p(x) = -x$ if $p\nmid x$ and $\Gamma_p(x+1)/\Gamma_p(x) = -1$ otherwise. It is known that $\Gamma_p(n+mp^{s+1}) \equiv \Gamma_p(n) \mod p^{s+1}$, for more details, see [Coh07]. From definition,

$$ n! = (-1)^n\Gamma_p(1+n)\cdot p^{[n/p]}([n/p])!. $$

Thus

$$\frac{\binom{2n}{n}}{\binom{2[n/p]}{[n/p]}} = p^{e(n)}\frac{\Gamma_p(1+2n)}{\Gamma_p(1+n)^2}, \tag{10}$$

where $e(n) = 0$ if the least nonnegative residue of n modulo p is smaller than $p/2$, otherwise, $e(n) = 1$. By properties of $\Gamma_p(x)$, for any positive integer k, the sequences

$$A(n) = B(n) = B^{(1)}(n) = \cdots = \binom{2n}{n}^4 \cdot \frac{1}{4^k} = \left(\frac{(\frac{1}{2})_n}{n!}\right)^k$$

satisfy all conditions of the Theorem 7. When $k = 2$, Theorem 7 implies that for λ in any unramified extension K of $\mathbb{Q}_p$ such that E_λ has ordinary reduction modulo p, there exists a unit $\alpha_{p,\lambda}$ in the ring of integers $\mathcal{O}_K$ of K such that

$$\frac{{}_2F_1\left(\begin{matrix}\frac{1}{2}, \frac{1}{2}\\ 1\end{matrix}; \lambda\right)_{p^s-1}}{{}_2F_1\left(\begin{matrix}\frac{1}{2}, \frac{1}{2}\\ 1\end{matrix}; \lambda^p\right)_{p^{s-1}-1}} \equiv \alpha_{p,\lambda} \pmod{p^s}. \tag{11}$$

Unlike $\beta_{p,\lambda}$ above, $\alpha_{p,\lambda}$ may vary if we replace λ by λ^p. However, $(-1)^{(p-1)/2}\beta_{p,\lambda} = \alpha_{p,\hat{\lambda}}$ where $\hat{\lambda}$ is the Teichmüller lift of λ modulo $p\mathcal{O}_K$ to $\mathcal{O}_K$. In fact, the discrepancy between (11) and (9) basically lies in the differences between the Witt operators and Hilbert operators. Using the result of Dwork and Ditters [Dit90], Kibelbek showed that if we let $A(n) = {}_rF_{r-1}\begin{bmatrix}\frac{1}{2} & \cdots & \frac{1}{2} \\ & 1 & \cdots 1\end{bmatrix}; \lambda\Bigg]_{n-1}$ then $\sum \frac{A(n)}{n}x^n$ is the logarithm of a 1-CFGL over $\mathbb{Z}[1/M][\lambda]$ for some integer M. In [KLMSY], an geometric interpretation of these 1-CFGLs was given explicitly based on [Sti87]. By relaxing the condition of $A(n) = B(n) = B^{(1)}(n) = \cdots$, Dwork's result implies that truncated hypergeometric series with rational upper parameters (and lower parameters to be all 1's) giving rise to CFGLs, integral at almost all primes, which are not necessarily 1-dimensional. It is natural to ask whether one can find isomorphic formal groups arising from an explicit algebraic equation. In fact, many of them are realized using hypersurfaces in weighted projective spaces, including many of geometric objects being Calabi-Yau manifolds. Meanwhile, for the untruncated hypergeometric series, they correspond to objects like periods, which we will illustrate using the Legendre family below.

5. ASD congruences, periods, differential equations, and related topics

5.1. **Periods, Picard-Fuchs equations, and modular forms.** A period of an elliptic curve E is an integral $\displaystyle\int_\gamma \frac{dx}{2y}$ over $\gamma \in H_1(E, \mathbb{Z})$. In general, these are transcendental numbers. For the Legendre family, the variation of the periods, $p(\lambda) = \int_{\gamma_\lambda} \frac{dx}{2\sqrt{x(x-1)(x-\lambda)}}$, are captured by its Picard-Fuchs (PF) equation alluded to in the previous section. Near 0, the unique (up to scalar multiple) homomorphic solution of this PF equation is ${}_2F_1\begin{bmatrix}\frac{1}{2} & \frac{1}{2} \\ & 1\end{bmatrix}; \lambda\Bigg]$. Thus $p(\lambda) = C \cdot {}_2F_1\begin{bmatrix}\frac{1}{2} & \frac{1}{2} \\ & 1\end{bmatrix}; \lambda\Bigg]$ for some constant C, which is known to be an algebraic multiple of π [BB87]. It is well-known that the Legendre family represents elliptic curves with 2-torsion points, whose moduli space $X(2)$ is parameterized by the classical modular lambda function $\lambda(z) := 16 \cdot \frac{\eta(2z)^4\eta(z/2)^2}{\eta(z)^6}$. When λ is viewed as a function of z, one has

$${}_2F_1\left[\begin{matrix}\frac{1}{2} & \frac{1}{2} \\ & 1\end{matrix}; \lambda(z)\right] = \theta_3^2(z), \tag{12}$$

where $\theta_3(z) = \sum_{n\in\mathbb{Z}} q^{n^2/2}$ with $q = e^{2\pi iz}$ is a Jacobi theta function of weight 1/2.

5.2. **Complex multiplication and results of Chowla-Selberg.** When the elliptic curve E has complex multiplication, i.e. its endomorphism ring R over $\mathbb{C}$ is an order of an imaginary quadratic field $K = \mathbb{Q}(\sqrt{-d})$ with fundamental discriminant $-d$, all periods are algebraic multiples of a transcendental number b_K, depending on K. The Selberg-Chowla formula [SC67] describes a choice of b_K:

$$b_K := \Gamma(1/2) \prod_{0<a<d} \Gamma(a/d)^{n\varepsilon(a)/4h}, \tag{13}$$

where n is the order of unit group in K, ε is a primitive quadratic Dirichlet character modulo d, and h is the class number of $\mathbb{Q}(\sqrt{-d})$.

Example 8. $b_{\mathbb{Q}(\sqrt{-4})} = \Gamma(1/2)\frac{\Gamma(\frac{1}{4})}{\Gamma(\frac{3}{4})} \sim \frac{\Gamma(\frac{1}{4})^2}{\Gamma(\frac{1}{2})}$, by the reflection formula $\Gamma(x)\Gamma(1-x) = \frac{\pi}{\sin(\pi x)}$. We use $\sim$ to mean up to an algebraic multiple.

Regard the invariant differential $\omega = \frac{dx}{2y}$ of E as an element of $H^1_{DR}(E,\mathbb{C})$, the dual of $H_1(E,\mathbb{Z})\otimes_{\mathbb{Z}}\mathbb{C}$. The endomorphism ring R of E over $\mathbb{C}$ acts on the 2−dimensional space $H^1_{DR}(E,\mathbb{C})$ with ω as a common eigenfunction of R. There is another common eigenfunction ν of R in $H^1_{DR}(E,\mathbb{C})$, defined over $\overline{\mathbb{Q}}$ and independent of ω. Chowla and Selberg further showed that the particular *quasi-period* $\int_\gamma \nu$ is an algebraic multiple of $2\pi i/b_K$, hence its transcendental part is also a Gamma quotient. Putting together, one obtains the relation

$$\int_\gamma \omega \cdot \int_\gamma \nu \sim \pi. \tag{14}$$

By §5.1, this number b_K also plays a role at singular values of modular forms. More precisely, for any weakly holomorphic (i.e. allowing poles at cusps) modular form F with integral weight k and algebraic Fourier coefficients, it is known that $F(\tau) \times (b_K/\pi)^{-k} \in \overline{\mathbb{Q}}$ for all $\tau \in K$ with $\Im(\tau) > 0$, see [Zag08].

5.3. **ASD congruences and Gross-Koblitz.** It is worth mentioning that Selberg-Chowla's results have p-adic analogues. Their formula (13) for b_K inspired the Gross-Koblitz formula [GK79]. Let $\pi_p \in \mathbb{C}_p$ be a fixed root of $x^{p-1} + p = 0$. Let φ be the Teichmüller character. The Gross-Koblitz formula states that under a suitable normalization, the Gauss sum

$$g(\varphi^{-j}) = -\pi_p^j \Gamma_p(\frac{j}{p-1}), \quad 0 \le j \le p-2. \tag{15}$$

Young gave another proof of the Gross-Koblitz formula using formal groups constructed from the Fermat curves [You94].

5.4. **ASD congruences and p-adic periods.** In some sense, ASD congruences also describes p-adic periods. To illustrate the idea, we use the following example of CM elliptic curve $E : y^2 = x^3 + x$, with endomorphism ring $R = \mathbb{Z}(\sqrt{-1})$ due to the order 4 automorphism $(x, y) \mapsto (-x, \sqrt{-1}y)$. If we expand $\frac{dx}{2y} = \sum a_n \xi^n \frac{d\xi}{\xi}$ with $\xi = \frac{-x}{y}$, the coefficients $a_n = 0$ for n even, and for n odd $a_n = \binom{\frac{n-1}{2}}{\frac{n-1}{4}}$ using the formula reviewed in §4.1. For prime $p \equiv 1 \mod 4$, E is ordinary, and the ASD congruence is reduced to 2-term: using (10) we have

$$\binom{\frac{np^r-1}{2}}{\frac{np^r-1}{4}} / \binom{\frac{np^{r-1}-1}{2}}{\frac{np^{r-1}-1}{4}} = \frac{\Gamma_p(\frac{1}{2} + np^r/2)}{\Gamma_p(\frac{3}{4} + np^r/4)^2} = \Gamma_p(\frac{1}{2} + np^r/2)\Gamma_p(\frac{1}{4} + np^r/4)^2, \quad \forall n \equiv 1 \mod 4.$$

As $r \to \infty$, we find the limit α_p in (7) is $\alpha_p = -\frac{\Gamma_p(1/4)^2}{\Gamma_p(\frac{1}{2})}$. This is a p-adic analogue of the period computed via Selberg-Chowla formula in Example 8.

5.5. **An example of weakly holomorphic differentials.** Consider the Fermat curve $E: x^3 + y^3 = 1$ with endomorphism ring $R = \mathbb{Z}[\frac{1-\sqrt{-3}}{2}]$. Two linearly independent eigenfunctions of R in $H^1_{DR}(E, \mathbb{C})$ are $\omega = \frac{dx}{y^2} = \sum_{n\geq 1} a_n x^n \frac{dx}{x}$, a holomorphic differential, and $\nu = \frac{xdx}{y} = \sum_{n\geq 1} b_n x^n \frac{dx}{x}$, a differential of second kind. At $p \equiv 1 \mod 3$, which are ordinary primes for E, we have

$$a_{p^n} = (-1)^{\frac{1}{3}(p^n-1)} \binom{-\frac{2}{3}}{\frac{1}{3}(p^n-1)} \quad \text{and} \quad b_{2p^n} = (-1)^{\frac{2}{3}(p^n-1)} \binom{-\frac{1}{3}}{\frac{2}{3}(p^n-1)}.$$

For details, see Example 6.3 of [Kat81]. By the discussion in §3, $a_{p^n}/a_{p^{n-1}} \equiv \alpha_p \mod p^n$ for all n, where α_p can be written in terms of p-adic Gamma product. However, numerical data seem to indicate deeper congruence relations:

$$a_{p^n} \equiv \alpha_p a_{p^{n-1}} \mod p^{2n}, \quad b_{2p^n} \equiv \frac{p}{\alpha_p} b_{2p^{n-1}} \mod p^{2n-1}. \tag{16}$$

5.6. **Another p-adic analogue of Selberg-Chowla relation, Ramanujan type congruences.** For the Legendre family, $H^1(E_\lambda, \mathbb{C})$ is generated by ω_λ, a holomorphic differential, and $\partial_\lambda \omega_\lambda$, see [Kat73]. Thus, the quasi-period of E_λ can be written as a linear combination of ${}_2F_1\left[\begin{matrix} \frac{1}{2} & \frac{1}{2} \\ & 1 \end{matrix}; \lambda\right]$ and $\partial_\lambda\, {}_2F_1\left[\begin{matrix} \frac{1}{2} & \frac{1}{2} \\ & 1 \end{matrix}; \lambda\right]$. Similar to (12), one can relate the quasi-period to an explicit weight -1 modular form. For details, see §3.4 of [CDLNS]. Using the well-known Clausen's formula

$${}_2F_1\left[\begin{matrix} 1-a & a \\ & 1 \end{matrix}; x\right]^2 = {}_3F_2\left[\begin{matrix} \frac{1}{2} & 1-a & a \\ & 1 & 1 \end{matrix}; -4x(x-1)\right], \tag{17}$$

one can express the formula (14) as

$$\sum_{k=0}^{\infty} \frac{(\frac{1}{2})_k^3}{k!^3} (-4\lambda(\lambda-1))^k (ak+1) = \frac{\delta}{\pi}, \tag{18}$$

for some computable algebraic numbers a, δ depending on λ when E_λ has complex multiplication. The derivation is given in [CDLNS]. Formulas of this type include

$$\sum_{k=0}^{\infty} \frac{(\frac{1}{2})_k^3}{k!^3} (6k+1) \frac{1}{4^k} = \frac{4}{\pi}$$

by Ramanujan. These so-called Ramanujan-type formulas for $1/\pi$ were first given by Borwein-Borwein [BB87] and Chudnovsky-Chudnovsky [CC88]. Later, van Hamme discovered several surprising p-adic analogues of Ramanujan formulas for $1/\pi$ [vH97]. For instance, he conjectured that for each prime $p > 3$

$$\sum_{k=0}^{\frac{p-1}{2}} \frac{(\frac{1}{2})_k^3}{k!^3} (6k+1) \frac{1}{4^k} \equiv \left(\frac{-1}{p}\right) p \mod p^4, \tag{19}$$

where $\left(\frac{\cdot}{p}\right)$ is the Legendre symbol. This conjecture was proved in [Lon11]. More generally, we have

Theorem 9 ([CDLNS])**.** *Given $\mu \in \overline{\mathbb{Q}}$ such that $\mathbb{Q}(\mu)$ is totally real and $|\mu| < 1$ for all embeddings, let $\lambda = \frac{1-\sqrt{1-\mu}}{2}$. Assume that the elliptic curve $E_\lambda : y^2 = x(x-1)(x-\lambda)$ has complex multiplication. Let a, δ be the algebraic numbers in (18) for E_λ. For each prime p unramified in $\mathbb{Q}(\sqrt{1-\lambda})$ such that (1) there is a maximal ideal $\wp$ of $\mathbb{Q}(\sqrt{1-\lambda})$ with residue field $\mathbb{Z}/p\mathbb{Z}$, (2) a, μ and the discriminant of E_λ are $\wp$-adic units, we have*

$$\sum_{k=0}^{p-1}\left(\frac{(\frac{1}{2})_k}{k!}\right)^3(ak+1)\mu^k \equiv \operatorname{sgn}\cdot\left(\frac{1-\lambda}{p}\right)\cdot p \mod \wp^2,$$

where $\left(\frac{1-\lambda}{p}\right)$ *is the Legendre symbol on the residue field of* $\wp$*, and* $\operatorname{sgn} = \pm 1$*, equal to* 1 *if and only if* p *is ordinary for* E_λ*.*

Meanwhile, numerical data suggest the following ASD type congruences, extending the conjecture by Zudilin which is the case $n = 1$:

$$\sum_{k=0}^{p^n-1}\left(\frac{(\frac{1}{2})_k}{k!}\right)^3(ak+1)\mu^k \equiv \operatorname{sgn}\cdot\left(\frac{1-\lambda}{p}\right)\sum_{k=0}^{p^{n-1}-1}\left(\frac{(\frac{1}{2})_k}{k!}\right)^3(ak+1)\mu^k\cdot p \mod \wp^{3n}. \tag{20}$$

5.7. **Supercongruences and complex multiplications.** In [CDE86], Chowla, Dwork, and Evans gave an improvement of the ASD congruence as follows: for $p \equiv 1 \mod 4$

$$\binom{\frac{p-1}{2}}{\frac{p-1}{4}} \equiv (-4)^{\frac{p-1}{4}}(a+bi) \mod p^2, \quad \text{where } p = a^2+b^2 \text{ with } a \equiv 1 \mod 4.$$

Such a congruence, which is stronger than what can be predicted by the theory of formal group, is called a *supercongruence*. Examples of supercongruences include (16) and (20) above. Here, we focus on the cases with complex multiplications. Using properties of the p-adic Gamma function, Coster [Cos88] was able to extend the above result to

$$\binom{\frac{p^r-1}{2}}{\frac{p^r-1}{4}}\Big/\binom{\frac{p^{r-1}-1}{2}}{\frac{p^{r-1}-1}{4}} \equiv (-4)^{\frac{p^{r-1}(p-1)}{4}}(a+bi) \mod p^{2r}, \quad p = a^2+b^2, a \equiv 1 \mod 4. \tag{21}$$

Coster and van Hamme have the following further generalization.

Theorem 10 (Coster and van Hamme, [CVH91])**.** *Let* p *be an odd prime and* d *a square-free positive integer such that* $(\frac{-d}{p}) = 1$*. Let* K *be an algebraic number field such that* $\sqrt{-d} \in K$ *and* $K \subset \mathbb{Q}_p$*. Consider the elliptic curve*

$$\mathcal{E} : Y^2 = X(X^2+AX+B)$$

with $A, B \in K$*, where* A *and* $\Delta = A^2 - 4B$ *are* p*-adic units. Let* ω *and* ω' *be a basis of periods of* $\mathcal{E}$*. Suppose that* $\tau = \omega'/\omega \in \mathbb{Q}(\sqrt{-d})$ *and* τ *has positive imaginary part. Let* $\wp, \bar\wp \in \mathbb{Q}(\sqrt{-d})$ *be complex conjugates such that* $\wp\bar\wp = p$*, with* $\bar\wp$ *a* p*-adic unit,* $\wp = u_1 + v_1\tau$*, and* $\wp\tau = u_2 + v_2\tau$ *with* u_1, v_1, u_2, v_2 *integers and* v_1 *even. Then we have*

$$P_{\frac{mp^r-1}{2}}\left(\frac{A}{\sqrt{\Delta}}\right) \equiv \varepsilon^{mp^{r-1}}\cdot\bar\wp\cdot P_{\frac{mp^{r-1}-1}{2}}\left(\frac{A}{\sqrt{\Delta}}\right) \mod \wp^{2r}, \tag{22}$$

where $P_k(x) = {}_2F_1\left[\begin{matrix}-k & 1+k \\ & 1\end{matrix}; \frac{1-x}{2}\right]$ *is the* k*th Legendre polynomial,* m *and* r *are positive integers, with* m *odd, and* $\varepsilon = i^{-u_2v_2+v_2+p-2}$*.*

In the heart of their proof lies a special Frobenius lifting that commutes with the endomorphism ring R of E. This Frobenius is a modification of the multiplication by $\wp$ map, which is a p-isogeny sending $t = -\frac{X}{Y}$ to a degree-p rational function of t. Using the above theorem and Clausen's formula (17), one has

Theorem 11 (Kibelbek, Long, Moss, Sheller, Yuan, [KLMSY])**.** *Let* $\lambda \neq 1$ *be an algebraic number such that* $\tilde E_\lambda : y^2 = (x-1)(x^2 - \frac{1}{1-\lambda})$ *has complex multiplications. Let* p *be a prime and suppose that* $\tilde E_\lambda$ *has a model defined over* $\mathbb{Z}_p$ *with good reduction modulo* $p\mathbb{Z}_p$*. Then*

$${}_3F_2\left[\begin{matrix}1/2 & 1/2 & 1/2 \\ & 1 & 1\end{matrix}; \lambda\right]_{\frac{p-1}{2}} = \sum_{k=0}^{\frac{p-1}{2}}\left(\frac{(\frac{1}{2})_k}{k!}\right)^3\lambda^k \equiv \left(\frac{\lambda-1}{p}\right)\alpha_{p,\lambda}{}^2 \mod p^2$$

where $\alpha_{p,\lambda}$ *is the unit root of* $X^2-[p+1-\#(\tilde{E}_\lambda/\mathbb{F}_p)]X+p=0$ *if* $\tilde{E}_\lambda$ *is ordinary at* p*; and* $\alpha_{p,\lambda}=0$ *if* $\tilde{E}_\lambda$ *is supersingular at* p*.*

As a corollary, one can deduce the following type of results that are difficult to prove directly.

Corollary 12. *For all primes* $p>3$*, we have*

$$\sum_{i=1}^{\frac{p-1}{2}}\binom{2i}{i}^3\sum_{j=1}^{i}\frac{1}{i+j}\equiv 0 \mod p. \tag{23}$$

Moreover, it is conjectured that the following ASD type congruences hold for ordinary prime $p>3$ and any $m,n\geq 1$

$$ {}_3F_2\left[\begin{matrix}1/2 & 1/2 & 1/2\\ & 1 & 1\end{matrix}\,;\,\lambda\right]_{\frac{mp^n-1}{2}}\equiv\left(\frac{\lambda-1}{p}\right){\alpha_{p,\lambda}}^2\,{}_3F_2\left[\begin{matrix}1/2 & 1/2 & 1/2\\ & 1 & 1\end{matrix}\,;\,\lambda\right]_{\frac{mp^{n-1}-1}{2}} \mod p^{2n}. \tag{24}$$

In [R-V01], Rodriguez-Villegas made several conjectures on supercongruences relating truncated hypergeometric series to Hecke eigenforms. Many of his conjectures have been proved and often the proofs rely on results like (23).

5.8. **ASD congruences and Fuchsian ordinary differential equations.** Apéry numbers play an important role in transcendence. Using them Apéry showed the irrationality of zeta values $\zeta(2)$ and $\zeta(3)$. Here, we will focus on the sequence $A(n)=\sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}$ that is related to $\zeta(2)$. This sequence satisfies several surprising ASD type congruences. In [Beu87], Beukers showed that for prime $p>3$,

$$A(mp^n-1)\equiv A(mp^{n-1}-1) \mod p^{3n}, \quad \forall m,n\geq 1. \tag{25}$$

In [SB85], Stienstra and Beukers proved that for prime $p>3$

$$A\Big(\frac{mp^n-1}{2}\Big)-a_pA\Big(\frac{mp^{n-1}-1}{2}\Big)+(-1)^{\frac{p-1}{2}}p^2A\Big(\frac{mp^{n-2}-1}{2}\Big)\equiv 0 \mod p^n, \quad \forall n\geq 1, \text{odd } m, \tag{26}$$

where a_p is the pth coefficient of $\eta(4z)^6$ that appeared before. Stienstra-Beukers conjectured that (26) holds mod p^{2n}. When $m=n=1$, the conjecture was proved by Ishikawa [Ish90] and Ahlgren [Ahl01].

Now we briefly explain the geometry behind the above results using the viewpoint of [Beu87]. It is well-known that $\sum_{n\geq 0}A(n)t^n$ satisfies an order-2 ordinary differential equation (ODE)

$$t(t^2-11t-1)\frac{d^2F(t)}{dt^2}+(3t^2-22t-1)\frac{dF(t)}{dt}+(t-3)F(t)=0. \tag{27}$$

In [Hon71], Honda asked "what algebraic differential equations 'yield' formal groups that are integral for almost all primes". Based on [Dwo69] Honda in [Hon72] constructed formal power series satisfying linear ODE that yield formal groups related to the Fermat curves. The coefficients of these power series are similar to the sequence used in (21). Honda's question concerns when a given linear Fuchsian (i.e. with regular singularities only) ODE $Lf=0$ arises from a Picard-Fuchs equation. A deep theorem of Katz says Picard-Fuchs equations are globally nilpotent, see [Kat70] for terminology and details. Let Σ denote the set of regular singularities of $Lf=0$. In particular, we restrict ourselves to degree-2 ODE. Recall that given such a Fuchsian ODE, one can construct a *monodromy representation*

$$\rho:\pi_1(\mathbb{C}P^1\setminus\Sigma,u_0)\to GL_2(\mathbb{C})$$

of the fundamental group $\pi_1(\mathbb{C}P^1\setminus\Sigma,u_0)$, where u_0 is any nonsingular point on the base curve [Yos87]. In particular, if $Im\rho$ can be embedded to $SL_2(\mathbb{R})$, then the image $Im\rho$ is a Fuchsian group [Shi71]. In this case, the local holomorphic solution of $Lf=0$ (under suitable assumption) is a weight-1 automorphic form of the Fuchsian group $Im\rho$, like (12), see [Sti85]. Upon knowing the local monodromy matrix at each singular point, one can tell whether $Im\rho$ has cusps or not.

One can further ask whether $Im\rho$ is *commensurable* with $SL_2(\mathbb{Z})$. When the ODE has only 3 singularities, i.e. being a hypergeometric differential equation, the answer is known due to classification of arithmetic triangular groups [Tak77]. Next in line are degree-2 ODEs with 4 singularities, like (27). For (27), the monodromy group $Im\rho$ is isomorphic to $\Gamma^1(5)$ mentioned in §2. The modular curve for $\Gamma^1(5)$ has genus 0 and we can pick as a Hauptmodul $t = \frac{E_2}{E_1} = q^{1/5} + \cdots$, where E_1, E_2 are weight-3 Eisenstein series for $\Gamma^1(5)$ that appeared in §2. Like (12), when we specify t as a modular function for $\Gamma^1(5)$, $\sum A(n)t^n$ is a weight-1 modular form and $\frac{dt}{dq^{1/5}}$ is a weight-2 modular form. Putting together one can verify that

$$\sum A(n)t^n \frac{dt}{t} = E_1 \frac{dq_5}{q_5}, \quad q_5 = q^{1/5}$$

where $E_1(z)$ is a Hecke eigenform for all Hecke operators T_p when $p > 5$ with 1 as an eigenvalue. Thus Beukers' result (25) modulo p^n can be explained via Proposition 3 as we are expressing $E_1 \frac{dq_5}{q_5}$ in terms of t, which is another local uniformizer at infinity. Meanwhile, we emphasize that the change of variable as described in Proposition 3 does not preserve supercongruences in general. See [CCS10] for some conjecture similar to (25) satisfied by Apéry like sequences.

To see (26) we adopt a similar view point. Let $t_2 = \sqrt{t}$. Thus $t_2 E_1 = \sqrt{E_1 E_2}$ is the weight-3 cusp form mentioned in §2. Then

$$t_2 E_1 \frac{dq_{10}}{q_{10}} = \sum A(n) t_2^{2n+1} \frac{dt_2}{t_2}, \quad q_{10} = q^{1/10}.$$

Motivated by Beukers results on Apéry numbers, Zagier [Zag09] did an extensive computer search for rational numbers a, b, λ such that the differential equation

$$(t(t^2 + at + b)F'(t))' + (t - \lambda)F(t) = 0 \tag{28}$$

has a solution in $\mathbb{Z}[[t]]$. Among his findings are cases where the monodromy groups are finite and ODEs equivalent to those of Hypergeometric series. The most interesting sporadic cases have 4 genuine singularities and infinite monodromy groups, in which case Zagier conjectured that the monodromy group is isomorphic to an index-12 subgroup of $SL_2(\mathbb{Z})$. His conjecture is actually implied by an earlier conjecture by Chudnovsky-Chudnovsky on special globally nilpotent Lamé ODE with 4 singularities, see [CC88, Conjecture 2].

6. Weight-k ASD congruences for noncongruence modular forms

As alluded to earlier, congruences that are stronger than what commutative formal group laws predict are harder to achieve, and their existence is usually due to extra symmetry like complex multiplication and/or special choice of the local uniformizer as well as the Frobenius lifting. However, in the realm of noncongruence modular forms of weight $k > 2$, one can always achieve supercongruence. This is due to the very special local uniformizer $q = e^{2\pi i z}$, the Frobenius lifting $q \mapsto q^p$ and their relation with the Gauss-Manin connection. For details, see Katz [Kat73].

6.1. **ASD congruences for weakly holomorphic modular forms.** Let Γ be a finite index subgroup of $SL_2(\mathbb{Z})$. Assume that the modular curve X_Γ has a model over $\mathbb{Q}$, the cusp at ∞ is a $\mathbb{Q}$-rational point with cusp width m. The completion of the local ring $\mathcal{O}_{X_\Gamma,\infty}$ at ∞ is isomorphic to $\mathbb{Q}[[t]]$ for some t satisfying $\delta t^m = q$ with $\delta \in \mathbb{Q}^\times$. Given a subring R of $\mathbb{C}$, let $M_k^{wk}(\Gamma, R)$ be the set of weakly holomorphic (i.e., holomorphic on the upper half-plane and meromorphic at cusps) weight k modular forms for Γ whose t-expansions at ∞ have coefficients in R. Denote by $S_k^{wk}(\Gamma, R)$ the submodule of functions in $M_k^{wk}(\Gamma, R)$ with vanishing constant term. A modular form $f \in M_k^{wk}(\Gamma, R)$ is called *weakly exact* if at each cusp c of Γ the Fourier coefficients $a_n(f, c)$ of f at c satisfy the condition $n^{-(k-1)}a_n(f, c)$ is integral over R for each $n < 0$. Write $S_k^{wk-ex}(\Gamma, R)$ (resp. $M_k^{wk-ex}(\Gamma, R)$) for the collection of weakly exact forms in $S_k^{wk}(\Gamma, R)$ (resp. $M_k^{wk}(\Gamma, R)$). Assume $k \geq 2$. Using equation (56) of [Zag08], one can verify that for $k \geq 2$, the linear map $D = q\frac{d}{dq}$ iterated $k-1$ times maps $M_{2-k}^{wk}(\Gamma, \mathbb{C})$ into $S_k^{wk-ex}(\Gamma, \mathbb{C})$.

Using geometric interpretations of weakly exact forms, Kazalicki and Scholl in [KS13] identified the quotient space $\frac{S_k^{wk-ex}(\Gamma,R)}{D^{k-1}(M_{2-k}^{wk}(\Gamma,R))}$ with the p-adic de Rham space $DR(\Gamma, R, k)$, which plays a key role in the proof of the Scholl congruence (4):

$$DR(\Gamma, R, k) = \frac{S_k^{wk-ex}(\Gamma, R)}{D^{k-1}(M_{2-k}^{wk}(\Gamma, R))}.$$

Similarly, they showed

$$DR(\Gamma, R, k)^* = \frac{M_k^{wk-ex}(\Gamma, R)}{D^{k-1}(M_{2-k}^{wk}(\Gamma, R))}.$$

As there are no holomorphic forms of negative weight, $S_k(\Gamma, R)$ is contained in $DR(\Gamma, R, k)$ and $M_k(\Gamma, R)$ in $DR(\Gamma, R, k)^*$. In fact, the following two short exact sequences hold:

$$0 \to S_k(\Gamma, R) \to DR(\Gamma, R, k) \to S_k(\Gamma, R)^\vee \to 0$$

and

$$0 \to M_k(\Gamma, R) \to DR^*(\Gamma, R, k) \to S_k(\Gamma, R)^\vee \to 0,$$

where $^\vee$ denotes the Serre duality. Suppose that $S_k(\Gamma, R)$ has R-rank $d = d(k)$. The above exact sequences imply that $DR(\Gamma, R, k)$ and $DR(\Gamma, R, k)^*$ are locally free R-modules of rank $2d$ and $2d$ plus the rank $d'(k)$ of the weight k Eisenstein series in $M_k(\Gamma, R)$, respectively.

It was shown in [ASD71] and [Sch85] that there is a positive integer M such that the d-dimensional space $S_k(\Gamma)$ has a basis consisting of functions whose t-expansions have coefficients in $R = \mathbb{Z}[\frac{1}{M}]$ and their q-expansions are integral over R. For any prime $p \nmid M$, we have R contained in $\mathbb{Z}_p$ (embedded in $\mathbb{C}$). Further, for $p > k-2$, there is an endomorphism ϕ_p on $DR(\Gamma, \mathbb{Z}_p, k)^*$ leaving $DR(\Gamma, \mathbb{Z}_p, k)$ invariant, arising from the Frobenius lifting originated in the map $q \mapsto q^p$ on Tate curve. Its characteristic polynomial $H_p(T)$ on $DR(\Gamma, \mathbb{Z}_p, k)$ lies in $\mathbb{Z}[T]$, where $H_p(T)$ coincides with the characteristic polynomial of the geometric Frobenius at p under the $2d$-dimensional Scholl representations recalled in §2. Thus all roots of $H_p(T)$ are algebraic integers with the same absolute value $p^{(k-1)/2}$, and they can be paired off as $\{\alpha, p^{k-1}/\alpha\}$ when k is even due to an alternating non-degenerate pairing on the ℓ-adic cohomology space. The characteristic polynomial of ϕ_p on the quotient $DR(\Gamma, \mathbb{Z}_p, k)^*/DR(\Gamma, \mathbb{Z}_p, k)$ also lies in $\mathbb{Z}[T]$, with all roots of absolute value 1 (cf. [Sch85, pp. 75]). Kazalicki and Scholl proved in [KS13] that the congruences (4) satisfied by the cusp forms in $S_k(\Gamma, \mathbb{Z}_p)$ also hold for weakly holomorphic forms in $M_k^{wk-ex}(\Gamma, \mathbb{Z}_p)$, although with weaker moduli. Since to study the behavior at another cusp amounts to replacing Γ by a conjugate, we only consider the cusp at infinity.

Theorem 13 (Kazalicki and Scholl [KS13])**.** *Let $p > k-1$ be a prime. Suppose $f = \sum a_n(f) q^{n/m}$ in $M_k^{wk-ex}(\Gamma, \mathbb{Z}_p)$ is annihilated by $h(\phi_p)$ for some polynomial $h(T) = \sum_{j=0}^r A_j T^j \in \mathbb{Z}[T]$ dividing the characteristic polynomial of ϕ_p on $DR(\Gamma, \mathbb{Z}_p)^*$. Then*

$$\sum_{j=0}^r A_j a_{n/p^j}(f) \equiv 0 \mod p^{(k-1)\mathrm{ord}_p n} \qquad \textit{for all } n \geq 1.$$

Example 14. The space $S_{12}^{wk-ex}(SL_2(\mathbb{Z}), \mathbb{Z})$ is a $\mathbb{Z}$-module spanned by $\Delta(z) = \sum_{n\geq 1} \tau_n q^n$ and

$$g(z) := E_4(z)^6/\Delta(z) - 1464 E_4(z)^3 = q^{-1} - 1432236q + 51123200q^2 + 39826861650q^3 + \cdots.$$

As is well-known, the Fourier coefficients τ_n of Δ satisfy the recursion

$$\tau_{np} - \tau_p \tau_n + p^{11} \tau_{n/p} = 0 \quad \text{for all } n \geq 1 \text{ and all primes } p.$$

Kazalicki and Scholl showed that, for every prime $p \geq 11$, the Fourier coefficients $a_n(g)$ of g satisfy

$$a_{np}(g) - \tau_p a_n(g) + p^{11} a_{n/p}(g) \equiv 0 \mod p^{11 \mathrm{ord}_p n} \quad \text{for all } n \geq 1.$$

6.2. **ASD congruences for holomorphic cusp forms.** The stronger congruences (4) satisfied by cusp forms $f \in S_k(\Gamma, \mathbb{Z}_p)$ established by Scholl in [Sch85] resulted from the fact that ϕ_p on $DR(\Gamma, \mathbb{Z}_p, k)$ actually sends $S_k(\Gamma, \mathbb{Z}_p)$ into $p^{k-1}DR(\Gamma, \mathbb{Z}_p, k)$. The extra multiple p^{k-1} accounts for the higher exponent in the moduli. More precisely, the Fourier coefficients $a_n(f)$ of f at the cusp ∞ satisfy the congruence

$$\sum_{j=0}^{2d} A_j a_{n/p^j}(f) \equiv 0 \mod p^{(k-1)(1+ord_p n)} \qquad \text{for all } n \geq 1.$$

J. Kibelbek in his thesis [Kib11] gave an interpretation of the above $(2d+1)$-term ASD congruences in terms of d-CFGLs for $k = 2$.

In general, due to the lack of effective Hecke operators, one does not know how to decompose the degree-$2d$ Scholl representations into a sum of degree-2 subrepresentations, as what happened for Deligne representations for congruence groups. However, if extra symmetries are present, then sometimes they can be used to break the Scholl representations. Accordingly, one can decompose Scholl's congruences into 3-term ASD congruences, resembling the congruence case. We demonstrate below a few cases where extra symmetries are used to obtain 3-term ASD congruences for almost all primes and (semi-)fixed basis. More examples can be found in [Lon08, FHLRV, HLV12, ALLL].

6.3. **Examples.** Let Γ_3 be an index-3 subgroup of $\Gamma^1(5)$ such that $t_3 := \sqrt[3]{t} = \sqrt[3]{E_2/E_1}$ is a Hauptmodul of the modular curve X_{Γ_3}. The space $S_3(\Gamma_3)$ is spanned by $g_1 = E_1 t_3$ and $g_2 = E_1 t_3^2$, both in $\mathbb{Z}[1/3][[q^{1/15}]]$.

Theorem 15 (Li, Long, Yang [LLY05]). *For any prime $p > 3$, the coefficients of $g_1 \pm \sqrt{-1}g_2 = \sum a_\pm(n)q^{n/15}$ satisfy*

$$a_\pm(np^r) - b_\pm(p)a_\pm(np^{r-1}) + \chi_{-3}(p)p^2 a_\pm(np^{r-2}) \equiv 0 \mod p^{2r}, \quad \textit{for } r, n \geq 1,$$

where $\sum_{n\geq 1} b_\pm(n)q^n$ are two weight-3 congruence newforms of level 27 and quadratic character χ_{-3} associated to $\mathbb{Q}(\sqrt{-3})$.

Next we consider the index-4 subgroup Γ_4 of $\Gamma^1(5)$ defined similarly using $t_4 = \sqrt[4]{E_2/E_1}$. Let S be the space generated by the two weight-3 cusp forms $h_1 = E_1 t_4$ and $h_3 = E_1 t_4^3$ for Γ_4. There is a compatible family of degree-4 sub-Scholl-representations of $G_\mathbb{Q}$ attached to S. Consider the following four weight-3 congruence cuspforms defined using the η function:

$$f_1(z) = \frac{\eta(2z)^{12}}{\eta(z)\eta(4z)^5} = \sum_{n\geq 1} a_1(n)q^{n/8}, \qquad f_3(z) = \eta(z)^5\eta(4z) = \sum_{n\geq 1} a_3(n)q^{n/8},$$

$$f_5(z) = \frac{\eta(2z)^{12}}{\eta(z)^5\eta(4z)} = \sum_{n\geq 1} a_5(n)q^{n/8}, \quad \text{and} \quad f_7(z) = \eta(z)\eta(4z)^5 = \sum_{n\geq 1} a_7(n)q^{n/8}.$$

Their linear combination

$$f = f(z) = f_1(z) + 4f_5(z) + 2\sqrt{-2}(f_3(z) - 4f_7(z)) = \sum_{n\geq 1} a(n)q^{n/8} \tag{29}$$

is an eigenform of the Hecke operators at odd primes and $f(8z)$ has level 256, weight 3, and quadratic character χ_{-4} associated to $\mathbb{Q}(i)$.

Theorem 16 (Atkin, Li, Long [ALL08]). *For each odd prime p, the space $S =< h_1, h_3 >$ has a basis depending on the residue of $p \mod 8$ satisfying the ASD congruence* (1) *at p as follows.*

1. *If $p \equiv 1 \mod 8$, then both h_1 and h_3 satisfy* (1) *with $A_p = sgn(p)a_1(p)$ and $\mu_p = 1$, where $sgn(p) = \pm 1 \equiv 2^{(p-1)/4} \mod p$;*
2. *If $p \equiv 5 \mod 8$, then h_1 (resp. h_3) satisfies* (1) *with $A_p = 4ia_5(p)$ (resp. $-4ia_5(p)$) and $\mu_p = -1$;*

(3) *If* $p \equiv 3 \mod 8$*, then* $h_1 \pm h_3$ *satisfy* (1) *with* $A_p = \pm 2\sqrt{-2}a_3(p)$ *and* $\mu_p = -1$*;*
(4) *If* $p \equiv 7 \mod 8$*, then* $h_1 \pm ih_3$ *satisfy* (1) *with* $A_p = \mp 8\sqrt{-2}a_7(p)$ *and* $\mu_p = -1$.

Here $a_1(p), a_3(p), a_5(p), a_7(p)$ *are the Fourier coefficients of the congruence forms* f_1, f_3, f_5, f_7 *defined above.*

In [Sch85] Scholl showed that if half of the roots of the characteristic polynomial $H_p(T)$ of ϕ_p are distinct p-adic units, then one can find a basis for $S_k(\Gamma)$ satisfying the 3-term ASD congruence. In his thesis J. Kibelbek constructed examples to show that the 3-term ASD congruence does not always hold [Kib12]. The following counter-example is due to him. A similar counter-example was given in [KS13].

Consider the genus 2 hyperelliptic curve X over $\mathbb{Q}$ with an affine equation $y^2 = x^5 + 1$. By Belyĭ's theorem, $X \simeq X_\Gamma$ for a finite index subgroup Γ of $SL_2(\mathbb{Z})$ whose cusp at infinity has cusp width 10. On X there are two linearly independent holomorphic differentials $\frac{dx}{2y}$ and $x\frac{dx}{2y}$. Expanding them at the cusp ∞ with respect to the uniformizer $q^{1/10}$ we get

$$\frac{dx}{2y} = f_1 \frac{dq^{1/10}}{q^{1/10}}, \qquad x\frac{dx}{2y} = f_2 \frac{dq^{1/10}}{q^{1/10}},$$

where, up to normalization by a constant multiple,

$$f_1 = q^{1/10} - \frac{8}{5}q^{6/10} - \frac{108}{5^2}q^{11/10} + \frac{768}{5^3}q^{16/10} + \frac{3374}{5^4}q^{21/10} + \cdots = \sum_{n\geq 1} a_n(f_1)q^{n/10}$$

and

$$f_2 = q^{2/10} - \frac{16}{5}q^{7/10} + \frac{48}{5^2}q^{12/10} + \frac{64}{5^3}q^{17/10} + \frac{724}{5^4}q^{22/10} + \cdots = \sum_{n\geq 1} a_n(f_2)q^{n/10}.$$

They generate the space $S_2(\Gamma)$ and the module $S_2(\Gamma, \mathbb{Z}[\frac{1}{5}])$.

The l-adic representations attached to $S_2(\Gamma)$ are the dual of the Tate modules on the Jacobian of X_Γ. At primes $p \equiv 1, 4 \mod 5$, the characteristic polynomial $H_p(T)$ of the Frobenius at p has two distinct roots which are p-adic units, and hence $S_2(\Gamma, \mathbb{Z}[\frac{1}{5}])$ contains a basis satisfying 3-term ASD congruence. However, for primes $p \equiv 2, 3 \mod 5$, $H_p(T) = T^4 + p^2$ has no roots which are p-adic units. At such primes both f_1 and f_2 satisfy the Scholl congruences

$$a_{mp^{n+2}}(f_i) + p^2 a_{mp^{n-2}}(f_i) \equiv 0 \mod p^{n+1} \quad (i = 1, 2), \quad \forall n, m \geq 1,$$

but no 3-term congruences exist. In other words, $S_2(\Gamma)$ contains no nonzero forms satisfying ASD congruences for $p \equiv 2, 3 \mod 5$.

The differentials of the second kind $x^2\frac{dx}{2y}$ and $x^3\frac{dx}{2y}$ on X give rise to two weakly holomorphic cusp forms

$$f_3 = q^{3/10} - \frac{24}{5}q^{8/10} + \frac{268}{5^2}q^{13/10} - \frac{2624}{5^3}q^{18/10} + \frac{24714}{5^4}q^{23/10} + \cdots = \sum_{n\geq 1} a_n(f_3)q^{n/10},$$

and

$$f_4 = q^{4/10} - \frac{32}{5}q^{9/10} + \frac{552}{5^2}q^{14/10} - \frac{7808}{5^3}q^{19/10} + \frac{97104}{5^4}q^{24/10} + \cdots = \sum_{n\geq 1} a_n(f_4)q^{n/10}.$$

Note that f_3 and f_4 are holomorphic at ∞ but have poles at other cusps. The four forms f_1, f_2, f_3, f_4 together span the space $DR(\Gamma, \mathbb{Z}[\frac{1}{5}], 2)$. It is straightforward to see that ASD congruences at primes $p \neq 5$ with weaker moduli are satisfied by four linearly independent forms in $DR(\Gamma, \mathbb{Z}[1/5], 2)$.

7. An application of ASD congruences

Congruence forms with algebraic Fourier coefficients are known to have bounded denominators. A folklore conjecture asserts that a cusp form for a finite index subgroup of $SL_2(\mathbb{Z})$ with algebraic Fourier coefficients is a congruence form if and only if its Fourier coefficients have bounded denominators. When the space $S_k(\Gamma)$ is 1-dimensional, as discussed before, the ASD congruences hold and the associated Scholl representations are modular. Using these facts, we established in [LL12] the conjecture for the 1-dimensional case.

Theorem 17 (Li and Long, [LL12]). *Suppose that the modular curve X_Γ of Γ has a model defined over $\mathbb{Q}$ so that the cusp at ∞ is $\mathbb{Q}$-rational, $k \geq 2$ and $S_k(\Gamma)$ is 1-dimensional. Then a form $f = \sum a_n(f) q^{n/\mu}$ in $S_k(\Gamma)$ with Fourier coefficients in $\mathbb{Q}$ has bounded denominators if and only if it is a congruence cusp form.*

We outline the idea of the proof. As f has bounded denominators, without loss of generality we may assume that $a_n(f) \in \mathbb{Z}$. Selberg [Sel65] proved that the Fourier coefficients of f satisfy the following bound for some constant C:

$$|a_n(f)| < Cn^{k/2-1/5}, \quad \forall n \geq 1. \tag{30}$$

Meanwhile, the Scholl representations attached to $S_k(\Gamma)$ are modular in the sense that its L-function coincides with the L-function of a weight-k congruence Hecke eigenform $g = \sum b_n q^n \in \mathbb{Z}[[q]]$ with character χ. The ASD congruence established by Scholl says that there is an integer M such that for $p \nmid M$

$$a_{np^s}(f) - b_p a_{np^{s-1}}(f) + \chi(p)p^{k-1} a_{np^{s-2}} \equiv 0 \mod p^{(k-1)(s+1)}, \quad \forall n \geq 1.$$

The left hand side is an integer bounded by a fixed constant multiple of $(np^s)^{k/2-1/5}$ for all n and s. Thus for fixed n and s large enough, the congruence becomes an equality. This implies that, after twisting by a suitable multiplicative character ψ of $\mathbb{Z}$ to get rid of multiples of small primes, we have $f_\psi(z) = \sum \psi(n) a_n(f) q^n$ and $g_\psi(z) = \sum \psi(n) b_n q^n$ agree. Since twisting by characters preserves the congruence/noncongruence property of modular forms, we conclude that f, which has bounded denominators, has to be a congruence form.

8. Another type of congruences

Let f be a meromorphic modular function with Fourier coefficients $c_n(f)$, i.e., $f = \sum_{n > -\infty} c_n(f) q^n$. Fix a prime p. For a positive integer m such that $c_{p^m}(f) \neq 0$, let $t_m(f, n) = c_{np^m}(f)/c_{p^m}(f)$. Atkin had done extensive investigation on the coefficients of the modular j-function $j(z) = q^{-1} + 744 + 196884q + \cdots$. In [Atk67], he proved that for $p = 11$,

$$c_{n11^m}(j) \equiv 0 \mod 11^m, \quad \forall m, n \geq 1, \tag{31}$$

extending results of Lehner for $p = 5, 7$.

Conjecture 18 (Atkin and O'Brein [AOB67] and Atkin [Atk68]). *For any prime $p \neq 13$,*

$$t_m(j, np) - t_m(j, n) t_m(j, p) + p^{-1} t_m(j, n/p) \equiv 0 \mod 13^m, \quad \forall n \geq 1 \tag{32}$$

and

$$t_m(j, 13n) - t_m(j, n) t_m(j, 13) \equiv 0 \mod 13^m, \quad \forall n \geq 1. \tag{33}$$

For a given prime p, the Atkin U_p-operator sends $f = \sum a_n q^n$ to $U_p(f) = \sum a_{pn} q^n$. Thus,

$$\frac{U_p^m(j - 744)}{c_{p^m}(j - 744)} = \sum_{n \geq 1} t_m(j - 744, n) q^n.$$

The above conjecture was proved by Koike [Koi73] and [Kat73, §3.13] by knowing repeated application of U_{13} to $j - 744$ leads to a single 13-adic Hecke eigenform. The other akin conjectures

of Atkin for primes $p \leq 23$ are similarly established by Guerzhoy [Gue06, Gue10]. Atkin's observations and U_p operator play important roles in the development of p-adic modular forms [Ser73, Dwo73, Kat73, Hid86, Col96, et al.].

Suppose that $f = \sum_{n>-\infty} c_n(f)q^n \in \mathbb{Z}_p((q))$ and $c_1(f)$ is a p-adic unit. If f satisfies 2-term ASD congruence like (7) at p, that is, there exists a p-adic unit α_p such that

$$c_{np^{m+1}}(f) \equiv \alpha_p c_{np^m}(f) \mod p^{m+1} \quad \text{for all } m \geq 0 \text{ and } n \geq 1,$$

then $c_{p^m}(f)$ is a p-adic unit for all $m \geq 0$ so that $t_m(f,n)$ are in $\mathbb{Z}_p$. In the congruence above we can replace α_p by $c_{p^{m+1}}(f)/c_{p^m}(f)$, and the resulting congruence is nothing but the congruence of the form (33):

$$t_m(f,pn) - t_m(f,n)t_m(f,p) \equiv 0 \mod p^{m+1}.$$

Kazalicki [Kaz11] observed that congruence of type (31) for $p = 2$ is satisfied by a family of noncongruence modular functions. Recently, the second author and Alyson Denies computed the following during Sage Day 46 for a weight-1 noncongruence form. By Sebbar [Seb02], the space of integral weight holomorphic modular forms for $\Gamma_1(5)$ is a graded algebra generated by two normalized weight-1 forms f_1, f_2 ([Seb02, pp. 302]), whose zeros are located at the cusps only. Let $f = \sqrt{f_1 f_2}$, which is a weight-1 noncongruence modular form. Our data suggest the following pattern:

Conjecture 19. *Let $p = 5$. Then for $f = \sqrt{f_1 f_2}$, $m \geq 1$ and odd $n \geq 1$, we have*

$$t_m(f,5n) \equiv t_m(f,n) \mod 5^{2m+4}.$$

References

[Ahl01] S. Ahlgren, *Gaussian hypergeometric series and combinatorial congruences*, Symbolic computation, number theory, special functions, physics and combinatorics (Gainesville, FL, 1999), Dev. Math., vol. 4, Kluwer Acad. Publ., Dordrecht, 2001, pp. 1–12.

[Atk67] A. O. L. Atkin, *Proof of a conjecture of Ramanujan*. Glasgow Math. J. 8 1967 14–32.

[Atk68] ———, *Congruences for modular forms*, Computers in Mathematical Research, North-Holland, Amsterdam (1968), 8–19.

[AL70] A. O. L. Atkin, and J. Lehner, *Hecke operators on* $\Gamma_0(m)$. Math. Ann. 185 1970 134–160.

[ALLL] A. O. L. Atkin, W. C. Li, Liu, T. and L. Long, *Galois representations with quaternion multiplication associated to noncongruence modular forms*,Trans. Amer. Math. Soc., to appear, arXiv:1005.4105

[ALL08] A. O. L. Atkin, W. C. Li, and L. Long, *On Atkin and Swinnerton-Dyer congruence relations (2)*, Math. Ann. 340 (2008), no. 2, 335–358.

[AOB67] A. O. L. Atkin, J.N. O'Brien, *Some properties of $p(n)$ and $c(n)$ modulo powers of 13*. Trans. Amer. Math. Soc. 126 (1967) 442–459.

[ASD71] A. O. L. Atkin and H. P. F. Swinnerton-Dyer, *Modular forms on noncongruence subgroups*, Combinatorics (Proc. Sympos. Pure Math., Vol. XIX, Univ. California, Los Angeles, Calif., 1968), Amer. Math. Soc., Providence, R.I., (1971), 1–25.

[BLS64] H. Bass, M. Lazard, and J.-P. Serre, *Sous-groupes d'indice fini dans SL(n, Z)*. Bull. Amer. Math. Soc. 70 (1964), 385–392.

[BMS67] H. Bass, J. Milnor, and J.-P. Serre, *Solution of the congruence subgroup problem for $SL_n (n \geq 3)$ and $Sp_{2n}(n \geq 2)$*, Pub. Math. IHES 33 (1967), 59-137.

[Bel79] G. V. Belyĭ, *Galois extensions of a maximal cyclotomic field*. (Russian) Izv. Akad. Nauk SSSR Ser. Mat. 43 (1979), no. 2, 267–276, 479.

[Ber94] G. Berger, *Hecke operators on noncongruence subgroups*, C. R. Acad. Sci. Paris Sér. I Math. 319 (1994), no. 9, 915–919.

[Beu87] F. Beukers, *Another congruence for the Apéry numbers*, J. Number Theory 25 (1987), no. 2, 201–210.

[Beu87] ———, *Another congruence for the Apéry numbers*. J. Number Theory 25 (1987), no. 2, 201–210.

[BB87] J. M. Borwein and P. B. Borwein, *Pi and the AGM*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons Inc., New York, 1987, A study in analytic number theory and computational complexity, A Wiley-Interscience Publication.

[CCS10] H.H. Chan, S. Cooper, F. Sica, *Congruences satisfied by Apéry-like numbers*. Int. J. Number Theory 6 (2010), no. 1, 89-97.

[CDLNS] S. Chisholm, A. Deines, L. Long, G. Nebe, H. Swisher *p-Adic Analogues of Ramanujan Type Formulas for $1/\pi$*. Mathematics. 2013; 1(1):9–30.

[CDE86] S. Chowla, B. Dwork, and Ronald Evans, *On the mod p^2 determination of* $\binom{(p-1)/2}{(p-1)/4}$, J. Number Theory 24 (1986), no. 2, 188–196.

[Col96] R. F. Coleman *Classical and overconvergent modular forms* Invent. Math. 124 (1996), no. 1-3, 215–241.

[CC88] D. V. Chudnovsky and G. V. Chudnovsky, *Approximations and complex multiplication according to Ramanujan*, Ramanujan revisited (Urbana-Champaign, Ill., 1987), Academic Press, Boston, MA, (1988), 375–472.

[Coh07] H. Cohen *Number theory.* Vol. II. Analytic and modern tools. Graduate Texts in Mathematics, 240. Springer, New York, (2007). xxiv+596 pp.

[Cos88] M.J. Coster, *Generalisation of a congruence of Gauss*. J. Number Theory 29 (1988), no. 3, 300–310.

[CVH91] M. J. Coster and L. Van Hamme, *Supercongruences of Atkin and Swinnerton-Dyer type for Legendre polynomials*, J. Number Theory 38 (1991), no. 3, 265–286.

[Del69] P. Deligne. Formes modulaires et représentations l-adiques, *Séminaire N. Bourbaki,* 1968–1969, exp. n^o 355, 139–172

[DFG04] F. Diamond, M. Flach and L. Guo, *The Tamagawa number conjecture of adjoint motives of modular forms.* Ann. Sci. École Norm. Sup. (4) 37 (2004), no. 5, 663–727.

[Dia77] J. Diamond The p-adic log gamma function and p-adic Euler constants. Trans. Amer. Math. Soc. 233 (1977), 321–337.

[DM03] L. V. Dieulefait, J. Manoharmayum, *Modularity of rigid Calabi-Yau threefolds over* $\mathbb{Q}$, Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001), 159–166, Fields Inst. Commun., 38, Amer. Math. Soc., Providence, RI, (2003).

[Dit76] B. Ditters, *Sur les congruences d'Atkin et de Swinnerton-Dyer*, C. R. Acad. Sci. Paris Sér. A-B 282 (1976), no. 19, Ai, A1131–A1134.

[Dit90] E. J. Ditters, *Hilbert functions and Witt functions. An identity for congruences of Atkin and of Swinnerton-Dyer type*, Math. Z. 205 (1990), no. 2, 247–278.

[Dwo69] B. Dwork, *p-adic cycles*, Inst. Hautes Études Sci. Publ. Math. (1969), no. 37, 27–115.

[Dwo73] ———, *The U_p operator of Atkin on modular functions of level 2 with growth conditions.* Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), pp. 5767. Lecture Notes in Math., Vol. 350, Springer, Berlin, 1973.

[FHLRV] L. Fang, Liqun, J.W. Hoffman, B. Linowitz, A. Rupinski, and H. Verrill, *Modular forms on noncongruence subgroups and Atkin-Swinnerton-Dyer relations.* Experiment. Math. 19 (2010), no. 1, 1–27.

[GK79] B.H. Gross, N. Koblitz, *Gauss sums and the p-adic* Γ*-function.* Ann. of Math. (2) 109 (1979), no. 3, 569–581.

[Gue06] P. Guerzhoy, *On a conjecture of Atkin for the primes 13, 17, 19, and 23.* Math. Res. Lett. 13 (2006), no. 4, 549–555.

[Gue10] ——— *On a conjecture of Atkin.* J. Reine Angew. Math. 639 (2010), 121–130.

[Haz78] M. Hazewinkel, *Formal groups and applications*, Pure and Applied Mathematics, vol. 78, Academic Press Inc. [Harcourt Brace Jovanovich Publishers], New York, (1978).

[HLV12] J.W. Hoffman, L. Long, Ling, and H. Verrill, *On l-adic representations for a space of noncongruence cuspforms.* Proc. Amer. Math. Soc. 140 (2012), no. 5, 1569–1584.

[Hid86] H. Hida, *Iwasawa modules attached to congruences of cusp forms*, Ann. Sci. École Norm. Sup. (4) 19 (1986), no. 2, 231–273.

[Hon68] T. Honda, *Formal groups and zeta-functions*, Osaka J. Math. 5 (1968), 199–213.

[Hon71] ———, *Differential equations and formal groups.* Seminar on Modern Methods in Number Theory (Inst. Statist. Math., Tokyo, 1971), Paper No. 16, 11 pp. Inst. Statist. Math., Tokyo, (1971).

[Hon72] ———, *Formal groups obtained from generalized hypergeometric functions.* Osaka J. Math. 9 (1972), 447–462.

[Ish90] T. Ishikawa, *Super congruence for the Apéry numbers*, Nagoya Math. J. 118 (1990), 195–202.

[Kat70] N. M. Katz, *Nilpotent connections and the monodromy theorem : applications of a result of Turrittin.* Publications Mathematiques de l'IHES, 39 (1970), p. 175-232

[Kat73] ———, *p-adic properties of modular schemes and modular forms*, Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1973, 69–190. Lecture Notes in Mathematics, Vol. 350.

[Kat81] ———, *Crystalline cohomology, Dieudonné modules, and Jacobi sums*, Automorphic forms, representation theory and arithmetic (Bombay, 1979), Tata Inst. Fund. Res. Studies in Math., vol. 10, Tata Inst. Fundamental Res., Bombay, 1981, 165–246.

[Kaz11] M. Kazalicki, *2-adic properties of modular functions associated to Fermat curves.* Proc. Amer. Math. Soc. 139 (2011), no. 12, 4265–4271.

[KS13] M. Kazalicki and A. J. Scholl, *Modular forms, de Rham cohomology and congruences*, arXiv:1301.5876, (2013)

[Kib11] J. Kibelbek, *Formal groups gnd Atkin And Swinnerton-Dyer congruences*, Ph.D. Thesis, The Pennsylvania State University, (2011).

[Kib12] ———, *On Atkin-Swinnerton-Dyer congruence relations for noncongruence subgroups*, Proc. Amer. Math. Soc., to appear.

[KLMSY] J. Kibelbek, L. Long, K. Moss, B. Sheller, and H. Yuan, *Supercongruences and complex multiplication*, arXiv1210:4489.

[KW09] C. Khare and J.-P. Wintenberger, *On Serre's conjecture for 2-dimensional mod p representations of* Gal($\overline{\mathbb{Q}}/\mathbb{Q}$), Ann. of Math. (2) 169 (2009), no. 1, 229–253.

[Kis09a] M. Kisin, *Modularity of 2-adic Barsotti-Tate representations*, Invent. Math. 178(3) (2009), 587–634.

[Koi73] M. Koike, *Congruences between modular forms and functions and applications to the conjecture of Atkin*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. 20 (1973), 129–169.

[Li75] W.-C. W. Li, *Newforms and functional equations*. Math. Ann. 212 (1975), 285–315.

[Li12] ———, *The arithmetic of noncongruence modular forms*, Fifth International Congress of Chinese Mathematicians. Part 1, 2, AMS/IP Stud. Adv. Math., 51, pt. 1, vol. 2, Amer. Math. Soc., Providence, RI, 2012, 253–268.

[LLY05] W. C. W. Li, L. Long, and Z. Yang, *On Atkin and Swinnerton-Dyer congruence relations*, J. of Number Theory 113 (2005), no. 1, 117–148.

[LL12] W.-C. W. Li and L. Long, *Fourier coefficients of noncongruence cuspforms*, Bull. Lond. Math. Soc. 44 (2012), no. 3, 591–598.

[Lon08] L. Long, *On Atkin and Swinnerton-Dyer congruence relations. III.* J. Number Theory 128 (2008), no. 8, 2413–2429.

[Lon11] ———, *Hypergeometric evaluation identities and supercongruences*, Pacific J. Math. 249 (2011), no. 2, 405–418.

[Mik71] T. Miyake *On automorphic forms on GL2 and Hecke operators*. Ann. of Math. (2) 94 (1971), 174–189.

[R-V01] F. Rodriguez-Villegas, *Hypergeometric families of Calabi-Yau manifolds*. Calabi-Yau varieties and mirror symmetry (Toronto, ON, 2001), 223–231, Fields Inst. Commun., 38, Amer. Math. Soc., Providence, RI, 2003

[Seb02] A. Sebbar, *Modular subgroups, forms, curves and surfaces*. Canad. Math. Bull. 45 (2002), no. 2, 294–308.

[Sel65] A. Selberg, *On the estimation of Fourier coefficients of modular forms*. 1965 Proc. Sympos. Pure Math., Vol. VIII 1–15 Amer. Math. Soc., Providence, R.I.

[SC67] A. Selberg and S. Chowla, *On Epstein's zeta-function*, J. Reine Angew. Math. 227 (1967), 86–110.

[Sch85] A. J. Scholl, *Modular forms and de Rham cohomology; Atkin-Swinnerton-Dyer congruences*, Invent. Math. 79 (1985), no. 1, 49–77.

[Ser73] J.P. Serre, *Formes modulaires et fonctions zêta p-adiques*. (French) Modular functions of one variable, III (Proc. Internat. Summer School, Univ. Antwerp, 1972), pp. 191–268. Lecture Notes in Math., Vol. 350, Springer, Berlin, (1973).

[SW99] C. M. Skinner and A. J. Wiles, *Residually reducible representations and modular forms,* Inst. Hautes Études Sci. Publ. Math. (1999), no. 89, 5-126 (2000).

[SW01] ———, *Nearly ordinary deformations of irreducible residual representations,* Ann. Fac. Sci. Toulouse Math. (6) 10 (2001), no. 1, 185–215.

[Shi71] G. Shimura, *Introduction to the arithmetic theory of automorphic functions*, Publications of the Math. Soc. of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo, (1971), Kanô Memorial Lectures, No. 1.

[Sti87] J. Stienstra, Formal group laws arising from algebraic varieties. *American Journal of Mathematics*, 109, no.5, (1987), 907-925.

[SB85] J. Stienstra and F. Beukers, *On the Picard-Fuchs equation and the formal Brauer group of certain elliptic $K3$-surfaces*, Math. Ann. 271 (1985), no. 2, 269–304.

[Sti85] P.F. Stiller, *A note on automorphic forms of weight one and weight three*. Trans. Amer. Math. Soc. 291 (1985), no. 2, 503–518.

[Tak77] K. Takeuchi, *Arithmetic triangle groups*. J. Math. Soc. Japan 29 (1977), no. 1, 91–106.

[Tho80] J. G. Thompson, *A finiteness theorem for subgroups of* PSL(2, $\mathbf{R}$) *which are commensurable with* PSL(2, $\mathbf{Z}$), The Santa Cruz Conference on Finite Groups (Univ. California, Santa Cruz, Calif., 1979), Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., Providence, R.I., (1980), 533–555.

[vH97] L. van Hamme, *Some conjectures concerning partial sums of generalized hypergeometric series*, p-adic functional analysis (Nijmegen, 1996), Lecture Notes in Pure and Appl. Math., vol. 192, Dekker, New York, 1997, 223–236.

[Yos87] M. Yoshida, Masaaki, *Fuchsian differential equations. With special emphasis on the Gauss-Schwarz theory.* Aspects of Mathematics, E11. Friedr. Vieweg & Sohn, Braunschweig, (1987). xiv+215 pp.

[You94] P. T. Young, *On the Gross-Koblitz formula*, Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993), Contemp. Math., vol. 168, Amer. Math. Soc., Providence, RI, (1994), 379–386.

[Zag08] D. Zagier, *Elliptic modular forms and their applications*, The 1-2-3 of modular forms, Universitext, Springer, Berlin, (2008), 1–103.

[Zag09] ———, *Integral Solutions of Apéry-like recurrence equations*, Groups and symmetries, CRM Proc. Lecture Notes, 47, Amer. Math. Soc., Providence, RI, (2009), 349–366.

Department of Mathematics, Pennsylvania State University, University Park, PA 16802, USA and National Center for Theoretical Sciences, Mathematics Division, National Tsing Hua University, Hsinchu 30013, Taiwan, R.O.C.

E-mail address: wli@math.psu.edu

Department of Mathematics, Cornell University, Ithaca, NY 14850, USA and Department of Mathematics, Iowa State University, Ames, IA 50011, USA

E-mail address: linglong@iastate.edu